Taming the IPv6 Address Space with Hyhoneydv6

Sven Schindler

Potsdam University
Institute for Computer Science
Operating Systems and Distributed Systems

WorldCIS-2015, Dublin, October, 2015

Outline

1 Introduction

2 Results from a /34 Darknet Experiment

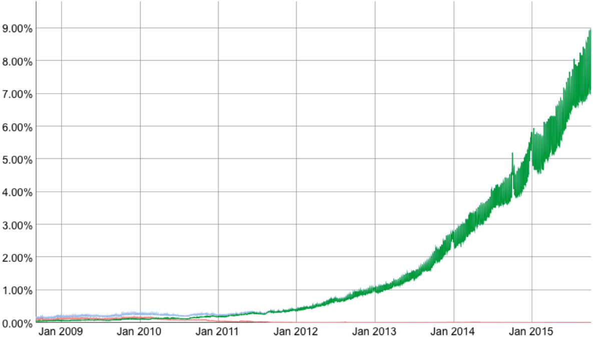
3 Hyhoneydv6: Requirements, Architecture and Features

4 Performance Measurements

5 Conclusion and Future Work

IPv6 is not fictional!

- **IPv6 traffic growth of more than 100 percent** over a single year[1]
- Some countries measure 33 percent IPv6 traffic



[1] http://www.google.com/intl/en/ipv6/statistics.html

Are there any IPv6 Attacks yet?

- Ullrich et al. [6] present an overview over IPv6 attacks
- Encounter **same threats as in IPv4**
- **New threats** through IPv6 design and IPv4/IPv6 transition mechanisms
- THC-IPv6[2] or SI6 IPv6 Toolkit[3] exploit IPv6 vulnerabilities

[2] https://www.thc.org/thc-ipv6/

[3] http://www.si6networks.com/tools/ipv6toolkit/

Facing Attacks with Honyepots

- Honeypots interact with attacker and allow us to analyse attacks
  - Low-interaction: service stubs or simulated services
  - High-interaction: authentic network services
  - Hybrid: combination of low- and high-interaction honeypot
- Two major low-interaction IPv6 honeypot projects
  - Dionaea - specialised in SIP and SMB
  - Honeydv6 - based on Honeyd[4], developed at the University of Potsdam
- **No high-interaction honeypot solution with focus on IPv6 available**

[4] http://www.honeyd.org

Outline

1 Introduction

2 Results from a /34 Darknet Experiment

3 Hyhoneydv6: Requirements, Architecture and Features

4 Performance Measurements

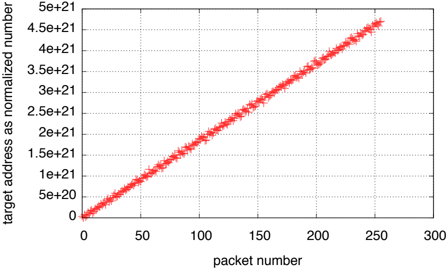
5 Conclusion and Future Work

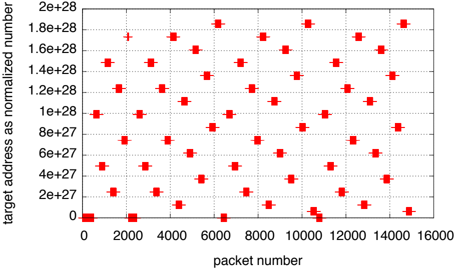
Results from a Darknet Experiment

- New and sophisticated **scanning approaches**?
- 15-months observation of an unused /34 address space
- Chance that a packet targets the darknet 1 : 17,179,869,184
- Only one in about $6 * 10^{23}$ addresses in our /34 network contacted
- Observed wide-range networks scans
- Mainly two scan patterns: linear and apparently random

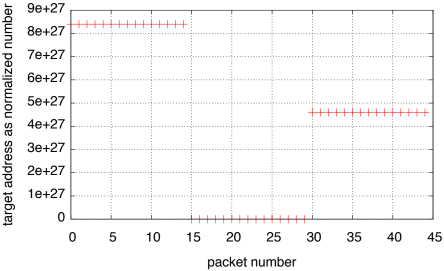
Total Packets	255,840	
ICMPv6	224,010	87.56%
TCP	31,604	12.35%
UDP	226	0.09%

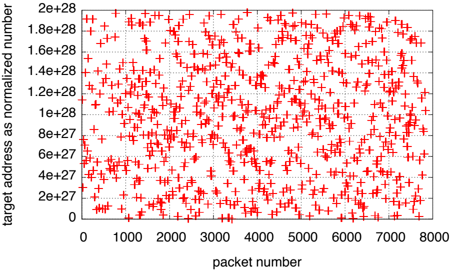
Scanning Pattern I





Scanning Pattern II





Outline

1 Introduction

2 Results from a /34 Darknet Experiment

3 Hyhoneydv6: Requirements, Architecture and Features

4 Performance Measurements

5 Conclusion and Future Work

IPv6 Honeypot Requirements

- **Genuine service emluation**
  - No service stubs
  - Provide protocols with encryption

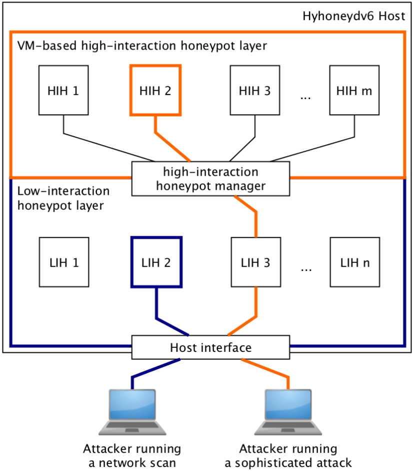
IPv6 Honeypot Requirements

- **Genuine service emluation**
  - No service stubs
  - Provide protocols with encryption
- **IPv6 address space coverage**
  - Brute force of IPv6 address space impossible [3]
  - Dynamic honeypot instantiation as provided by Honeydv6

IPv6 Honeypot Requirements

- **Genuine service emluation**
  - No service stubs
  - Provide protocols with encryption
- **IPv6 address space coverage**
  - Brute force of IPv6 address space impossible [3]
  - Dynamic honeypot instantiation as provided by Honeydv6
- **Price/Performance**
  - Require few machines
  - No cloud-based solutions

Hyhoneydv6 Architecture


Hyhoneydv6 Host
VM-based high-interaction honeypot layer
HIH 1
HIH 2
HIH 3
...
HIH m
high-interaction honeypot manager
Low-interaction honeypot layer
LIH 1
LIH 2
LIH 3
...
LIH n
Host interface
Attacker running a network scan
Attacker running a sophisticated attack

Major Hyhoneydv6 Features

- Dynamic instantiation of high-interaction honeypots
- Remote address configuration
- Transparent TCP proxy

Features - Dynamic Instantiation

- Network scans handled by low-interaction honeypots
- Attacks on network services handled by high-interaction honeypots
- QEMU-based high-interaction honeypot [2]
- Libvirt to control the machines [7]
- **New high-interaction honeypot manager** prepares libvirt configuration
- Machines maintained in pool which is initialised on startup

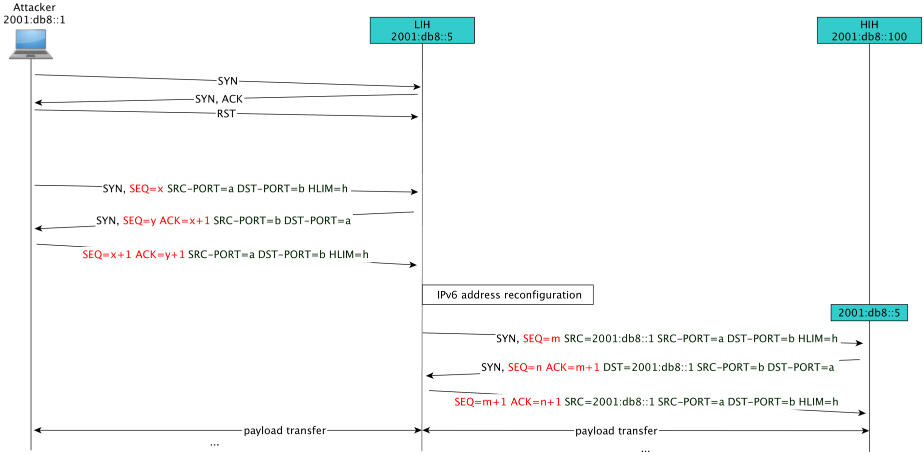
Features - Remote IPv6 Address Configuration

- Machine addresses require reconfiguration for attack
- Different approaches considered: DHCPv6, OS modifications, remote login, custom configuration server
- **Configuration server** is fast and avoids OS modifications
- High-interaction honeypot manager connects to configuration server and triggers IPv6 configuration for requested destination

Features - Transparent TCP Proxy

- Connections need to be handed over to high-interaction honeypots transparently
- **New proxy mechanism** implemented which forwards traffic between attacker and high-interaction honeypot
- High-interaction honeypots isolated via network bridge
- Proxy adopts requested address, ports and hop limits

TCP-Handoff



Attacker
2001:db8::1

LIH
2001:db8::5

HIH
2001:db8::100

SYN

SYN, ACK

RST

SYN, SEQ=x SRC−PORT=a DST−PORT=b HLIM=h

SYN, SEQ=y ACK=x+1 SRC−PORT=b DST−PORT=a

SEQ=x+1 ACK=y+1 SRC−PORT=a DST−PORT=b HLIM=h

IPv6 address reconfiguration

2001:db8::5

SYN, SEQ=m SRC=2001:db8::1 SRC−PORT=a DST−PORT=b HLIM=h

SYN, SEQ=n ACK=m+1 DST=2001:db8::1 SRC−PORT=b DST−PORT=a

SEQ=m+1 ACK=n+1 SRC=2001:db8::1 SRC−PORT=a DST−PORT=b HLIM=h

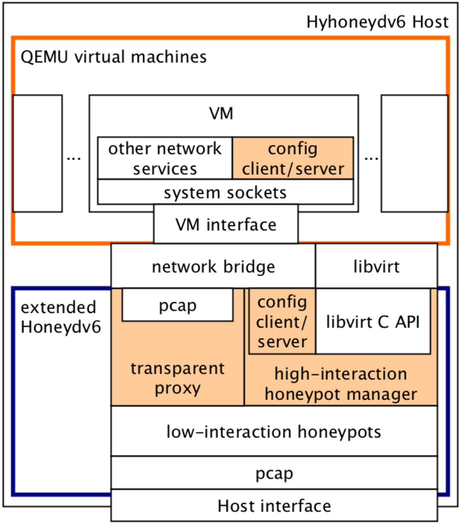
payload transfer

...

payload transfer

...

Internal Architecture Overview



Outline

1 Introduction

2 Results from a /34 Darknet Experiment

3 Hyhoneydv6: Requirements, Architecture and Features

4 Performance Measurements

5 Conclusion and Future Work

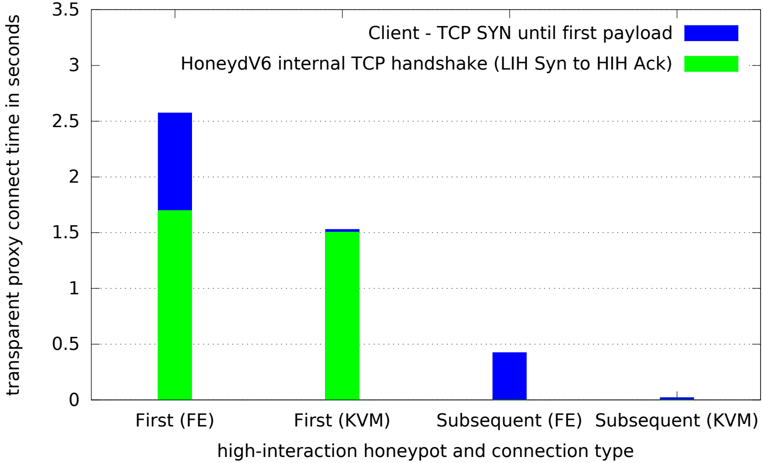
Host Hardware Specifications

Device/System	Specification
Operating system	Ubuntu 12.04 LTS
Qemu	1.0
Motherboard	EP45-DS3
CPU	Intel(R) Core(TM)2 Quad CPU Q9550 @ 2.83GHz
Memory	4GB (2x2) 800 MHz
Network	RTL8111/8168/8411 PCI Express GE Ctrl. (r8169 Gigabit Ethernet driver 2.3LK-NAPI)
HD	SanDisk SDSSDP25 (read: 490MB/s write: 350MB/s)

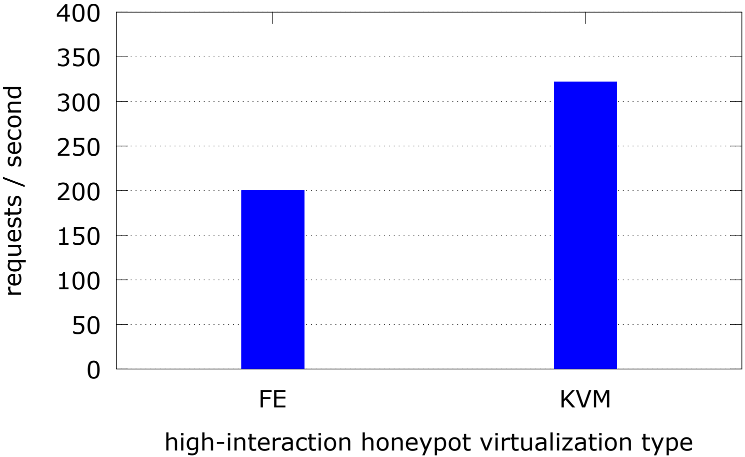
VM Specifications

Device/System	Specification
Operating systems	Debian 7.5 kern. 3.2.0-4-686 pae
Memory	256 MB
Network	Realtek Semiconductor, RTL-8139/8139C/8139C
CPU	QEMU virtual CPU

Connect Time



Requests per Second



Outline

1 Introduction

2 Results from a /34 Darknet Experiment

3 Hyhoneydv6: Requirements, Architecture and Features

4 Performance Measurements

5 Conclusion and Future Work

Conclusion

- Darknet experiment reveals wide-ranging IPv6 network scans
- First hybrid honeypot system for IPv6 networks
  - Dynamic Honeypot Instantiation
  - Address Reconfiguration
  - Transparent Proxy
- Simulate entire IPv6 networks with high-interaction honeypots on a single host
- Performs well on off-the-shelf hardware

Future Work

- Integration of Hyhoneydv6 into production networks
- Improve logging facilities
- Future open source project:
  https://redmine.cs.uni-potsdam.de/projects/honeydv6/wiki

Thank you

Time for questions and suggestions...

References

[1] Michael D. Bailey, Evan Cooke, David Watson, Farnam Jahanian, and Niels Provos.
A Hybrid Honeypot Architecture for Scalable Network Monitoring.
Technical Report CSE-TR-499-04, University of Michigan, Ann Arbor, Michigan, USA, October 2004.

[2] Fabrice Bellard.
Qemu, a fast and portable dynamic translator.
In *Proceedings of the Annual Conference on USENIX Annual Technical Conference*, ATEC '05, pages 41–41, Berkeley, CA, USA, 2005. USENIX Association.

[3] T. Chown.
IPv6 Implications for Network Scanning.
RFC 5157 (Informational), March 2008.

[4] Patrice Clemente, Jean-François Lalande, and Jonathan Rouzaud-Cornabas.
HoneyCloud: elastic honeypots - On-attack provisioning of high-interaction honeypots.
In *International Conference on Security and Cryptography*, pages 434–439, Rome, Italy, July 2012.

[5] Xuxian Jiang and Xuxian Jiang Dongyan.
Collapsar: A vm-based architecture for network attack detention center.
In *In Proceedings of the 13th USENIX Security Symposium*, pages 15–28, 2004.

[6] Johanna Ullrich and Katharina Krombholz and Heidelinde Hobel and Adrian Dabrowski and Edgar Weippl.
Ipv6 security: Attacks and countermeasures in a nutshell.
In *8th USENIX Workshop on Offensive Technologies (WOOT 14)*, San Diego, CA, 2014. USENIX Association.

[7] M Tim Jones.
Anatomy of the libvirt virtualization library.
IBM developer Works, pages 97–108, 2010.

[8] Georgios Portokalidis, Asia Slowinska, and Herbert Bos.
Argos: an Emulator for Fingerprinting Zero-Day Attacks.
In *Proc. ACM SIGOPS EUROSYS'2006*, Leuven, Belgium, April 2006.

[9] N. Provos and T. Holz.
Virtual Honeypots: From Botnet Tracking to Intrusion Detection.
Addison-Wesley, 2008.

[10] Michael Vrable, Justin Ma, Jay Chen, David Moore, Erik Vandekieft, Alex C. Snoeren, Geoffrey M. Voelker, and Stefan Savage.
Scalability, fidelity, and containment in the potemkin virtual honeyfarm.
In *Proceedings of the Twentieth ACM Symposium on Operating Systems Principles*, SOSP '05, pages 148–162, New York, NY, USA, 2005. ACM.